# Law Relating To Cyber Terrorism-

# A Comparative Study of Existing Laws at National and International Level

**Summary Report**

**Submitted to the**

**Faculty of Law**

**Mody Institute of Technology & Science**

**For the Award of Degree of**

**Doctor of Philosophy**

**In**

**Law**


**Supervisor/ Advisor:**

**Prof. Satish C. Shastri**

**Dean, Faculty of Law**

**Mody Institute of Technology & Science**

**Submitted by:**

**Shobhna Jeet**

**Enrolment No. 090732**


**2011**

# Summary

## Brief Summary of the Study: Major Observations

Today there are various general threats to the world at large and individual in society. Climate change, ozone depletion, deforestation, global warming, terrorism, war, crime and cyber crime are the some of the general threats for the era of technology and science. The cyber terrorism is the powerful threat that has come out from general threat i.e. cyber crime (menace to the whole world). These crimes committed with the use of information systems are threat to the information based economies of the world's leading countries like India. The information infrastructure has become a critical part of the backbone of our economies. The security of these computer and communication systems and their protection against computer crime are therefore of essential importance. The spreading of computer technology into almost all areas of life as well as the interconnection of computers by international computer networks have made computer crime more diverse, more dangerous, and internationally present in the form of cyber terrorism. The security of these computer and communication system and their protection against computer crime are therefore of essential importance.

The borderless nature of the Internet poses a dilemma. Internet sites cannot function if they must conform to the varying legal requirements of every jurisdiction in the world. Standards of permissible advertisements, political speech, religious liberty and religious expression, and even permissible hate speech and discussion of drug use vary widely between nations and cultures. Complying with each of these standards would impose untenable compliance costs and burdens on portals and websites alike. The various national laws show remarkable differences, especially with respect to the criminal law provisions on hacking, trade secret protection and illegal content. Considerable differences also exist with respect to the coercive powers of investigative agencies (especially with respect to encrypted data and investigations in international networks), the range of jurisdiction in criminal matters, and with respect to the liability of intermediary service providers on the one hand and content providers on the other hand. Computers and the internet present new ways to engage in old crimes, such as fraud and piracy. They also have made it possible for criminals to perpetrate new harmful acts, like data access and interference. For these reasons, countries around the world are taking measures to combat computer crime. However, national laws and regional agreements alone are not sufficient to address the global nature of cyber terrorism. Therefore, in order to prosecute cyber terrorism as well as other types of computer crime, a common international framework must be created that can punish these crimes irrespective of where they are

committed. Without the proper legal and enforcement infrastructure, cyber terrorism will engulf the global business.

**Objectives:**

The most deadly and destructive consequence of our dependency on technology is a reason of the emergence of concept of "cyber terrorism". The broad objective of the study is to explore various laws in different countries (including India) to cope up this problem. In light of this, the present study intends to achieve the following objectives: To define the concept of terrorism, cyber-crime and cyber terrorism. i) To describe the history of cyber terrorism in relation to the cyber-crime. ii) To explain the concept of cyber forensic and deliberate on the functioning of cyber forensic. iii) To discuss the international conventions dealing with the cyber-crimes. iv) To state the laws relating to cyber terrorism in UK, USA, Pakistan and India. v) To highlight the legal regimes and judicial approach in India to manage the cyber terrorism.

The work began with the discussion of the conversion of traditional terrorism to cyber terrorism. The transgression of technology put computers in peril. ICT (Information and Communication technology) revolution of course has a positive impact upon the economic growth of our country. In the cyber age, ICT is benefitting billion across the world by bridging certain gaps and multiplying human potential in every walk of life. The internet has revolutionized the way business approach and conduct work. For consumers, the idea of purchasing online is appealing for several reasons. A well designed and implemented e-commerce system can lower transaction costs, reduce inefficiencies, promote better information flow, and encourage better cooperation between buyers and sellers. In today's rapidly changing world of e- commerce, almost anything can be bought over the internet and delivered right to one's front door. By transcending international boundaries, the internet and the World Wide Web enable the company to market and deliver products and services to customers located in target countries often thousands of miles away efficiently and cost effectively. With little more than a click of a mouse, business can communicate, engage in commerce, and expand their business opportunities. At the same time, there are certain social, political, and economic implications being observed globally either in the form of 'spying websites' like wiki leaks hacking activities and decryption of data. The global character of digital space, internationally spread services, and the global development of social network sites go hand in hand with the emerging international crime networks raising serious challenges to the existing social, political and economic set up. There emerges a clash

between personal development and economic prosperity, and sustained security of humans. The trust citizen use to have in society and government to protect their pace, safety and prosperity gets eroded by the threats posed before us by the advanced Information Technology. Thus this work has tried to develop a means to restrict the transgression of criminal activities by cyber criminals.

Eradicating cyber terrorism is a means of strengthening international peace and security. To develop the uniform laws, conventions and treaties at international level is need of the hour. Our national laws regarding such crimes have covered a long distance from Information Technology Act, 2000 to the Information Technology Amendment Act 2008. With that amendment a single section has been added for cyber terrorism i.e. 66F provide life sentence against cyber terrorism. There are some solutions that are available in Information Technology Act 2000; Examples are the amendment in the Information Technology Act, 2000. The Act provides for Digital signatures (The term "digital signature" has been replaced with "electronic signature" to make the Act more technology neutral by the 2008 amendment Act), under Chapter III, which may be considered functional equivalent to physical world signatures capable of meeting all the fundamental requirements, like authenticity of the sender, message integrity and non-repudiation for making the electronic records legally binding. Thus the Information Technology Act, 2000 acts as an enabling Act. By providing the provisions to prosecute the cyber crime offenders, the Act functions as a regulating Act. The Act demarcates the cyber contraventions from cyber offences and provides separate redressal mechanisms for both. The Sections 63 and 64 of the IT Act, 2000(as amended by amendment Acts of 2006 and 2008) deals with the cyber contraventions. The Sections 65 to 67C of the Act deals with the cyber offences. The Act also seeks to fight terrorism. In view of the increasing threat of terrorism in the country, the 2008 Amendment to the Act has included an amended Section 69 giving power to the state to issue directions for interception or monitoring of decryption of any information through any computer resource. Further, Sections 69 A and B, two new sections, grant power to the state to issue directions for blocking for public access of any information through any computer resource and to authorize to monitor and collect traffic data or information through any computer resource for cyber security.

Over the period of time, computer network kept growing larger and larger and now it fulfills a wide variety of requirement including information, education and even entertainment. Internet function as a pocket switching network in which the information to be transmitted is

broken into small pockets of bit that can be transmitted as capacity of the particular connection allows. These pockets are labeled with the address of their final destination and may follow any number of different routes from computer to computer and before it reaches to final destination where the same is again resembled into the originally transmitted information. The peculiarity with internet is there is no central authority or system that regulates traffic across the Internet. There is no one to govern the Internet; there is no one to permit entry or no one to complain when things go wrong, thus making it a true network of networks. Since there is no authority to control, it allows persons to use it the way they want. The criminals are misusing this great medium for their nefarious activities, which led to a genre of crimes known as Cyber crime. The legal complexities increased after the emergence of internet. According to black's law dictionary jurisdiction is defined as the power of court to decide a matter in controversy and presupposes the existence of a duly constituted court with the control over the matter and parties. All sovereign states possess jurisdiction over all persons and things within its territorial limits and all causes, civil or criminal, arising within these limits. This definition was applicable to the traditional concept of jurisdiction. Now, cyber space has no physical boundaries. It is an ever-growing exponent and dynamic space. Internet is allowing the transmission of a data without human intervention. Its automatic ability to re-route the data on any available network and also that the internet uses packet switching protocol make the jurisdictional determination in a cyber crime prosecution more complex. Thus it is suggested that a law to deal with the jurisdiction of crimes committed under cyberspace can be enacted to stop the enhancement of the boundaries of cyberspace.

The convention on cyber crime declared almost all Cyber crimes like offences against confidentiality, integrity and availability of computer data and system, computer related forgery, fraud, child pornography as extraditable. India is not a signatory of this convention but section 75 of IT Act 2000 states about the extra-territorial application of this Act. The only proviso is offence or contravention involves, computer system or computer network situated in India. The procedure of 'letter regulatory' (section 166A and section 166B of the Criminal Procedure Code.) Enables investigation of crime in a foreign country is not easy and hopelessly out of tune with the scope of computer crime. Even section 188 of Criminal Procedure Code requires prior permission of the central government to inquire into or try offences committed outside India, which puts shackles on investigation agency's work. American court has been successful in interpreting the personal jurisdiction principle in online scenario. Indian law system is in harmony with other legal system and definitely gives



Shobhna Jeet

due credence to the private international law and conflict of law approaches. In India, emphasis is still on "cause of action" principle. Hence it is suggested that Indian judiciary, if needed can borrow the principles laid down by U.S. judiciary as a persuasive means but not at the cost of established 'Indian' principles.

Computer forensics is used to identify evidence when personal computers are used in the commission of crimes or in the abuse of company policies. Computer forensic tools and procedures are also used to identify computer security weaknesses and the leakage of sensitive computer data. In the past, documentary evidence was typically stored on paper and copies were made with carbon paper or photocopy machines. Most documents are now stored on computer hard disk drives, floppy diskettes, zip disks, and other forms of removable computer storage media. Computer forensics deals with Ending, extracting, and documenting this form of electronic documentary evidence. It is an ongoing battle to stay up with the criminals; new challenges require new skills and knowledge. In relation to training, much more needs to be done to ensure that all law enforcement personnel have a basic understanding of search and seizure issues in relation to electronic evidence, there is also a need for more advanced and ongoing training for those involved in the investigation of electronic crime and for specialist training for a cadre of expert staff involved in the forensic computing area. Investigators involved in the investigation of complex e-crime will require some essential forensic computing skills and knowledge. Many e- crimes of the future will be traditional crimes simply perpetrated through the use of ICT. Many offenders will leave their footprints in cyberspace and new skills and techniques will be required to enable the criminal justice system to deal with the e-crime issue and prevent its occurrence. As far as the criminal law is concerned, computer forensic does not provide any provision. So it is suggested to ensure that our laws are well positioned to deal with the new and unique challenges of policing cyberspace.

At international level attempts have been made to combat the menace of cyber crime and cyber terrorism. In recent years, certain international bodies, such as the Council of Europe, the organization for Economic Co-operation and Development (OECD) or the G8 conference, have begun to consider cyber security and cyber crime issues as part of their policy agenda. On the one hand, it is believed that the problems of crime using computers will rarely require the creation of new substantive criminal law; rather, they suggest need for better and effective enforcement of existing laws through international cooperation. It is suggested that crimes in cyberspace should be regulated the same way as those in real space as computer is merely an



Shobhna Peer

instrument. On the other hand, it is believed that marked differences exist between cyber crimes and conventional crime. Cyber crimes are grossly under-detected and under-reported. The laws in the area are complicated, and are evolving at a different rate from the underlying technology. As a result, responding to attacks against computers and information systems, such as malicious hacking, dissemination of viruses, and denial of service attacks poses serious problems. This view therefore requires addressing the issue of cyber crimes by evolving specific legislations and conventions.

As developing countries are jumping onto the bandwagon, penetration of Internet and awareness is on an overall low level. Different National Governments in Asia have yet to galvanize themselves into action vis-à-vis Internet and cyberspace. The future holds tremendous promise for Asia and Asian countries have to respond to the same with lightening speed. The problem is nonetheless that many have neither the expertise nor the experience to deal with the legal and policy issues necessary. International Telecommunications Union has helped certain developing countries to become actively involved in the deployment and use of services aimed at building security and trust, thereby extending the benefits of ICTs beyond commercial to societal applications such as government and health. U.S. has passed felony statutes criminalizing violation of international accords dealing with international radio or wire communications. Maliciously interfering with satellite transmissions is a felony in the U.S., similar to wire fraud. Therefore it may be suggested that these statutes could be expanded to include external and internal cyber attacks that do not reach the level of an armed attack. In this way, the U.S. terrorism statutes, which define terrorism as "committing acts constituting crimes under the law of any country to intimidate or coerce a civilian population; to influence government policy by intimidation or coercion; or to affect the conduct of government by mass destruction, assassination, or kidnapping," could be used to further criminalize the various forms of cyber attacks.

The Pakistan market has now grown manifolds with the majority of internet users in Karachi and then Lahore and Islamabad. These three cities jointly provide over 90 percent of the customer base and expansion in activity is also likely to remain primarily confined to these cities because of the concentration of economic activity in these cities. Pakistan has a legal framework in place to address cyber crimes. The Electronic Transaction Ordinance 2002 was passed by Pakistan Government with the objective to recognize and facilitate documents, records, information, communications and transactions in electronic form, and to provide for the accreditation of certification service providers. With this legal framework we do have



Shabbir Ahmed

legal backing for electronic information and communication, as any written and signed document. Furthermore, the Electronic Crime Act 2004 was prepared by the Ministry of Information Technology, Pakistan with the Electronic Transaction Ordinance 2002 as the basis. The Act addresses and lays down legislative terms for the following cyber crimes: Criminal access, Criminal data access, Data damage, System damage, Electronic fraud, Electronic forgery, Misuse of devices, Misuse of encryption, Malicious code, Cyber stalking, Spamming, Spoofing, Unauthorized interception, Cyber Terrorism, Waging cyber war, Enhanced punishment for offences involving sensitive electronic systems, Attempt and aiding or abetting. It is not possible to eliminate cyber crime from the cyber space in its entirety. However, it is quite possible to check it. Any legislation in its entirety might be less successful in totally eliminating crime from the globe. The primary step is to make people aware of their rights and duties (to report crime as a collective duty towards the society) and further making the application of the laws more stringent to check crime. Developing nations must learn from the experiences of developed nations and leap forward to prepare against the inevitable cyber crime. It is suggested that in order to strengthen the overall infrastructure, efforts by each country must be made at an international level to cooperate and coordinate with each other so as to come too harmonized terms on matters regarding security. In this regards, international instruments such as the Council of Europe's Convention on Cyber Crime 2001, could prove extremely valuable in fighting cyber crime at an international level. However, in any draft legislation it is important that the provisions of the cyber law are not made so stringent that it may retard the growth of the industry and prove to be counter-productive. Although the term "cyber terrorism" is absent from the terminology of the Indian law, Section 69 of the Information Technology Act is a strong legislative measure to counter the use of encryption by terrorists. This section authorizes the Controller of Certifying Authorities (CCA) to direct any Government agency to intercept any information transmitted through any computer resource.

Terrorism has immensely affected India. The reasons for terrorism in India may vary vastly from religious to geographical to caste to history. The Indian Supreme Court took a note of it in *Kartar Singh v. State of Punjab*, where it observed that the country has been in the firm grip of spiraling terrorist violence and is caught between deadly pangs of disruptive activities. Apart from many skirmishes in various parts of the country, there were countless serious and horrendous events engulfing many cities with blood-bath, firing, looting, mad killing even without sparing women and children and reducing those areas into a graveyard, which brutal



Shobhna Jeet

atrocities have rocked and shocked the whole nation Deplorably, determined youths lured by hard-core criminals and underground extremists and attracted by the ideology of terrorism are indulging in committing serious crimes against the humanity. Presently there are established laws that govern the "Terrorism" in cyber Space. However, there are no special laws governing "Cyber Terrorism". On October 17, 2000 special laws governing Cyber Crimes became effective in India with the passage of Information Technology Act 2000 (ITA-2000). Subsequently, the special act for Terrorism, POTA was also enacted with effect from 24th October 2001. Hence it is suggested that we need to therefore look at the laws governing "Cyber Terrorism" within these laws and any other associated legislation that may come into effect by cross reference including the IPC. Terrorism in Meta Space using Cyber space as a conduit is to be governed by the laws of the Meta space such as POTA with evidence gathered from Cyberspace as per the provisions of ITA-2000 which brought in some changes in the Indian Evidence Act, on the other hand, "Terrorism" in Cyber Space is a different aspect. Unfortunately, when ITA 2000 was enacted, the focus of legislation was not on "Cyber Terrorism". ITA 2000 therefore addresses some issues of Cyber Crimes but does not adequately address the issues of "Cyber Terrorism"

Cyber crimes raise new issues for legal systems. As Procedure and Evidentiary Law Relating to Cyber Terrorism in India are concerned countries need penal laws that adequately address cyber crime. Maximum either developed or developing countries do not have penal laws adequate to deal with cyber crime. An analysis is more problematic when one turns to procedural law, since there is much more variation among nations in this area. Notwithstanding that, it is important at least to note how procedural law may need to be revised to facilitate the investigation and apprehension of cybercriminals. After all a country can have a comprehensive penal code that reaches every known variety of cyber crime but still be unable to prosecute cybercriminals because of gaps in its procedural law. Therefore it is suggested that legislative responses to cyber crime should be both rigorous and conservative. They should be rigorous in evaluating the legal system's existing ability to deal with cyber crime, but they should be conservative in taking steps to improve that ability.

Internet is a cooperative venture not owned by a single entity or government, there are no centralized rules or laws governing its use the absence of geographical boundaries may give rise to a situation where the act legal in one country where it is done may violate the laws of another country. This process further made complicated due to the absence of a uniform and harmonized law governing the jurisdictional aspects of disputes arising by the use of Internet.

In addition to establishing a connecting nexus, traditional international doctrine also calls for a "reasonable" connection between the offender and the forum. Depending on the factual context, courts look to such factors, as whether the activity of individual has a "substantial and foreseeable effect" on the territory, whether a "genuine link" exists between the actor and the forum, the character of the activity and the importance of the regulation giving rise to the controversy, the extent to which exceptions are harmed by the regulation, and the importance of the regulation in the international community. So it is suggested that the traditional jurisdictional paradigms may provide a framework to guide analysis for cases arising in cyberspace. It must be noted that by virtue of section 1(2) read with section 75 of the Information Technology Act, 2000 the courts in India have "long arm jurisdiction" to deal with cyber terrorism.

The social infrastructure is the base for the economic growth of any country. The government policies, rules, regulations and the institutions that enforce the social infrastructure is a primary determinant of the extent to which individuals are willing to make the long term investment in capitals, skills, and technology that are associated with long run economic success. So the basic changes in the social infrastructure of the economy: changes in the government policies and institutions that make up the economic environment of these economies.

Cyber terrorism is becoming a menace for India and India has to be sound to tackle the same technologically and legally as well. There is dire need to amend the Information Technology Act, 2000 (IT Act, 2000) in this regard as a single provision is not sufficient as per the cyber law experts .Even there is no national ICT crisis management plan of India that is addressing the menace of cyber terrorism in India. Securing the critical national infrastructure of India from cyber attacks should be a priority area for India. This requires formulating a cyber security policy of India that is presently missing. Without a cyber security policy and strategy of India, the cyber security initiatives of India are directionless. Even there is no legal framework for cyber security in India. By incorporating a few ineffective and irrelevant provisions in the IT Act 2000, Indian government thinks that it has the cyber security law in India. Apart from this plethora of sections there are some suggested solutions that have been drawn after this research Likewise the borderless liaisons of IT revolution have made the police work more intricate. They are not acquainted with the modern technology to trace out the culprit. They require some training programme to get it with. Moreover the police stations are not well equipped to face such type of emergencies. This is the dire need of the hour to

improve all major police station of the city. These are the solution that can be applied on the grass root level.

Cyber forensics is a tool to identify evidence when personal computers are used in commission of crime but there is no specific law available to deal with it. Provisions related to cyber forensics may be inserted in the criminal laws like Indian Penal Code and Indian Evidence Act 1872. As far as the conventions on this issue are concerned unite actions at International level may be taken. International cooperation in cyber crime investigation in the form of mutual legal assistance requires an international agreement or other similar arrangement such as reciprocal legislation. Such provisions, whether multilateral or bilateral, oblige the authorities of a contracting party to respond to a request for mutual legal assistance in the agreed cases. Such assistance generally refers to specific coercive powers concerning the investigation of cyber crime. Apart from requests for traditional help, such as interviewing witnesses, the purpose is to obtain certain data stored in a computer system that is located in the territory of another state or being transferred electronically through a network and capable of being monitored or intercepted in the territory of that state.

The judiciary can play its vital role by adopting a stringent approach towards the menace of cyber terrorism. Firstly, it must tackle the jurisdiction problem because before executing its judicial powers the courts are required to satisfy themselves that they possess the requisite jurisdiction to deal with the situation. The absence of geographical boundaries may give rise to a situation where the act legal in one country where it is done may violate the laws of another country. Since the Internet is a cooperative venture not owned by a single entity or government, there are no centralized rules or laws governing its use. American court has been successful in interpreting the personal jurisdiction principle in online scenario. Indian law system is in harmony with other legal system and definitely gives due credence to the private international law and conflict of law approaches. In India, emphasis is still on "cause of action" principle. Indian judiciary, if needed can borrow the principles laid down by U.S. judiciary as a persuasive means but not at the cost of established 'Indian' principles.